Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it contains a valid OMB control number.

Substitute for form 1449A/PTO	Complete if Known		
	Application Number	09/390,362	
INFORMATION DISCLOSURE	Filing Date	09-07-1999	
STATEMENT BY APPLICANT	First Named Inventor	VANSTONE, SCOTT	
/ 5 %\	Art Unit	2766	
(use as many sheets as necessary)	Examiner Name	Not Yet Assigned	
Sheet 1 Sof 2	Attorney Docket Number		

	1	MACENA		U.S. PATE	NT DOCUMENTS	
Examiner		Document Number		Publication Date	Name of Patentee or	Pages, Columns, Lines, Where Relevant
	Cite No.1	Number	Kind Code (if known)	MM-DD-YYYY	Applicant of Cited Document	Passages or Relevant Figures Appear
		US-				<u> </u>
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		US-				
		us-				
		us-				RECEIVED
		us-				NECEIVED
		US-				JUL 1-5 2002
		US-				JUL 1 5 7007
		US-				
		US-				Technology Center 210
		US-				
		US-				
		US-				<u> </u>
		US-				

	FOREIGN PATENT DOCUMENTS							
Examiner Initials	Cite No.1	Office <sup>3</sup>	Foreign Patent Do Number4	Kind <sup>5</sup> (if known)	Publication Date MM-DD-YYYY	Name of Patentee or Applicant of Cited Document	Pages, Columns, Lines, Where Relevant Passages or Relevant Figures Appear	T€
O.K.		wo	01 10078	Al	02-08-2001	Coron et al	pg5, ln14 - pg7, ln7.	
9.A.		EP	0 639 907	Al	02-22-1995	R3 Security Engineering	col3 - col5, figs1,2.	
								ļ
								$\vdash$
		1				<del>                                     </del>		T

	70	
Examiner	dely adopte	Date d 603
Signature	F 13 0	Considered 81903

Burden Hour Statement: This form is estimated to take 2.0 hours to complete. Time will vary depending upon the needs of the individual case. Any comments on the amount of time you are required to complete this form should be sent to the Chief Information Officer, Patent and Trademark Office, Washington, DC 20231. DO NOT SEND FEES OR COMPLETED FORMS TO THIS ADDRESS. SEND TO: Assistant Commissioner for Patents, Washington, DC 20231.

<sup>\*</sup>EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

<sup>&</sup>lt;sup>1</sup> Applicant's unique citation designation number (optional). <sup>2</sup> See Kinds Codes of USPTO Patent Documents at <u>www.uspto.gov</u> or MPEP 901.04. <sup>3</sup> Enter Office that issued the document, by the two-letter code (WIPO Standard ST.3). For Japanese patent documents, the indication of the year of the reign of the Emperor must precede the serial number of the patent document. Kind of document by the appropriate symbols as indicated on the document under WIPO Standard ST. 16 if possible. Applicant is to place a check mark here if English language Translation is attached.

PTO/SB/08B (10-01)
Approved for use through 10/31/2002. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE

Under the Paperwork Reduction Act of 995, no persons and quired to respond to a collection of information unless it contains a valid OMB control number.

Attorney Docket Number

Substitute for form 1449B/PTO

JUL 1 2 2002 INFORMATION DISCL STATEMENT BY

Complete if Known 09/390,362 **Application Number** Filing Date 09-07-1999 **First Named Inventor** VANSTONE, SCOTT Group Art Unit 2766 **Examiner Name** Not Yet Assigned

(use as many sheets as necessary) Sheet of 2

	OTHER PRIOR ART NON PATENT LITERATURE DOCUMENTS					
Examiner Initials	Cite No.1	Include name of the author (in CAPITAL LETTERS), title of the article (when appropriate), title of the item (book, magazine, journal, serial, symposium, catalog, etc.), date, page(s), volume-issue number(s), publisher, city and/or country where published.	T <sup>2</sup>			
0. A.		CORON, JS., NACCACHE, D., STERN, J.P., "On the Security of RSA Padding", Advances in Cryptology CRYPTO'99, Proceedings of the 19th Annual International Cryptology Conference, August 19, 1999, Pages 1-18, Springer-Verlag, Berlin, Germany.				
0-A-		NYBERG, K. ET. AL., "Message Recovery for Signature Schemes Based on the Discrete Logarithm Problem", Designs, Codes and Cryptography, 1996, Pages 61-81, Vol. 7, No. 1-2, Kluwer Academic Publishers, Boston, U.S.				
O.A.		"ISO/IEC FCD 9796-1: Digital signature schemes giving message recovery. Part 1: Mechanisms using redundancy." ISO/IEC JTC1/SC27, July 7, 1999, No. 2352, Berlin, Germany.				
i						
			:			

Examiner Date Signature Considered

<sup>\*</sup>EXAMINER: Initial if reference considered, whether or not citation is in conformance with MPEP 609. Draw line through citation if not in conformance and not considered. Include copy of this form with next communication to applicant.

Applicant's unique citation designation number (optional). <sup>2</sup>Applicant is to place a check mark here if English language Translation is attached.